

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/US05/004502

International filing date: 10 February 2005 (10.02.2005)

Document type: Certified copy of priority document

Document details: Country/Office: US
Number: 60/543,777
Filing date: 11 February 2004 (11.02.2004)

Date of receipt at the International Bureau: 17 March 2005 (17.03.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

1293641

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

March 08, 2005

THIS IS TO CERTIFY THAT ANNEXED HERETO IS A TRUE COPY FROM THE RECORDS OF THE UNITED STATES PATENT AND TRADEMARK OFFICE OF THOSE PAPERS OF THE BELOW IDENTIFIED PATENT APPLICATION THAT MET THE REQUIREMENTS TO BE GRANTED A FILING DATE.

APPLICATION NUMBER: 60/543,777

FILING DATE: February 11, 2004

RELATED PCT APPLICATION NUMBER: PCT/US05/04502



Certified by

Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

Please type a plus sign (+) inside this box → ☐

PTO/SB/16 (5-03)
Approved for use through 04/30/2003. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PROVISIONAL APPLICATION FOR PATENT COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION FOR PATENT under 37 CFR 1.53(c).

PTO
22264 U.S. PTO
60/548777

INVENTOR(S)					
Given Name (first and middle (if any))		Family Name or Surname		Residence (City and either State or Foreign Country)	
Kelvin H.		Wildman		Honeoye Falls, NY	
Terri P.		Cleveland		Holley, NY	
David A.		Furth		Skaneateles, NY	
William		Becker		Little Silver, NJ	
<input type="checkbox"/> Additional inventors are being named on the _____ separately numbered sheets attached hereto					
TITLE OF THE INVENTION (280 characters max)					
BIOMETRIC SAFE LOCK					
Direct all correspondence to: CORRESPONDENCE ADDRESS					
<input type="checkbox"/> Customer Number		<input type="text"/>		<div>Place Customer Number Bar Code Label here</div>	
OR Type Customer Number here					
<input checked="" type="checkbox"/> Firm or Individual Name		JAECKLE FLEISCHMANN & MUGEL, LLP			
Address		39 State Street			
Address		Suite 200			
City		Rochester	State	NY	ZIP 14614-131-
Country		USA	Telephone	(585) 262-3640	Fax (585) 262-4133
ENCLOSED APPLICATION PARTS (check all that apply)					
<input checked="" type="checkbox"/> Specification		Number of Pages		<input type="checkbox"/> CD(s), Number	
		22		<input type="text"/>	
<input checked="" type="checkbox"/> Drawing(s)		Number of Sheets		<input checked="" type="checkbox"/> Other (specify)	
		7		Certif of Mailing EV386956743US	
<input type="checkbox"/> Application Data Sheet. See 37 CFR 1.76					
METHOD OF PAYMENT OF FILING FEES FOR THIS PROVISIONAL APPLICATION FOR PATENT (check one)					
<input type="checkbox"/> A check or money order is enclosed to cover the filing fees				FILING FEE AMOUNT (\$)	
<input checked="" type="checkbox"/> The Director is hereby authorized to charge filing fees or credit any overpayment to Deposit Account Number		10-0223		\$160.00	
<input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.					
The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.					
<input checked="" type="checkbox"/> No.					
<input type="checkbox"/> Yes, the name of the U.S. Government agency and the Government contract number are: _____					

Respectfully submitted,

SIGNATURE

TYPED or PRINTED NAME Dennis B. Danella, Esq.

TELEPHONE

(585) 262-3640

Date

2/11/2004

REGISTRATION NO.

46,653

(if appropriate)

Docket Number:

89843.027204

USE ONLY FOR FILING A PROVISIONAL APPLICATION FOR PATENT

This collection of information is required by 37 CFR 1.51. The information is used by the public to file (and by the PTO to process) a provisional application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 8 hours to complete, including gathering, preparing, and submitting the complete provisional application to the PTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Mail Stop Provisional Application, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

P19LARGE/REV05

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)Applicant(s): **Kelvin H. Wildman, et al**

Docket No.

89843.027204

Serial No.

TBA

Filing Date

Herewith

Examiner

TBA

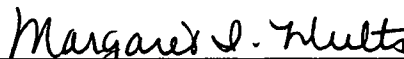
Group Art Unit

TBAInvention: **BIOMETRIC SAFE LOCK**

I hereby certify that the following correspondence:

Specification, Claims and Abstract (22 pages)*(Identify type of correspondence)*

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

February 11, 2004*(Date)***Margaret I. Hults***(Typed or Printed Name of Person Mailing Correspondence)**(Signature of Person Mailing Correspondence)***EV 386956743 US***("Express Mail" Mailing Label Number)***Note: Each paper must have its own certificate of mailing.**

CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)Applicant(s): **Kelvin H. Wildman, et al**

Docket No.

89843.027204

Serial No.

TBA

Filing Date

Herewith

Examiner

TBA

Group Art Unit

TBAInvention: **BIOMETRIC SAFE LOCK**

I hereby certify that the following correspondence:

Seven (7) Sheets of Informal Drawings (identified)*(Identify type of correspondence)*

is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR 1.10 in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on

February 11, 2004*(Date)***Margaret I. Hults***(Typed or Printed Name of Person Mailing Correspondence)**(Signature of Person Mailing Correspondence)***EV 386956743 US***("Express Mail" Mailing Label Number)***Note: Each paper must have its own certificate of mailing.**

BIOMETRIC SAFE LOCK

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] Not applicable.

STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT

[0002] Not applicable.

BACKGROUND OF THE INVENTION

[0003] The present invention relates to a biometric lock for a safe or other type of enclosure. In particular, the present invention is directed to a lock mechanism that utilizes a unique identifying characteristic of an individual in determining whether to allow access to an internal compartment of a safe. More particularly, the present invention is directed to a biometric safe lock that includes visual cues such as an instruction display, a crosshair identifier, and prompt Lighting Emitting Diodes (LED's) that are associated with a biometric sensor to assist the user in using the biometric safe lock. Furthermore, the present invention includes a locking mechanism for securing administrative access to the biometric lock.

[0004] It is known to use a biometric safe lock for securing various types of enclosures. For instance, known biometric safe locks may use a person's fingerprint to allow access to the interior portion of a safe or other type of enclosure. In order to gain access to the interior of the enclosure, a user places his or her finger on a fingerprint sensor, the biometric lock interprets the information gathered from the sensor and determines whether or not the gathered fingerprint information is associated with an authorized user of the safe lock. If the safe lock does not recognize the information gathered by the sensor, it will deny access to the safe and the lock will remain in a locked

position. If the lock recognizes the information gathered by the sensor, the locking mechanism is moved to an opened position to allow access to the user to access the interior compartment of the safe.

[0005] However, known biometric locks present a number of drawbacks and deficiencies. For instance, these biometric safe locks do not provide any guidance to the user for properly positioning the fingerprint on the sensor. Improper finger positioning on the sensor makes it difficult for the sensor to properly read and interpret the users fingerprint. If the sensor cannot read the fingerprint because of improper positioning, the lock will deny access to the user and the user will be required to restart the access procedure without knowing how his or her fingerprint should be positioned on the sensor.

[0006] Another problem with prior art biometric locks is that the user may have a difficult time understanding what to do during the process of unlocking the biometric lock. Known biometric safe locks commonly utilize sounds, such as beeps, to instruct the user on how to proceed. Solely using audible indicators may be confusing to the user and may require the user to refer to the operating instruction manual to determine the meaning of the audible indicators, which may be a time consuming process.

[0007] Further, known biometric safe locks may include an administrator button that is located on an interior portion of the safe, which may be used to add or delete one or more authorized fingerprints stored in the biometric lock. In particular, the administrator button is typically located in an exposed location within the interior of the safe. Therefore, the administrator button may be utilized by anyone with access to the safe. Allowing access to the administrator button to anyone with access to the safe may be problematic since any of the users of the safe may use the administrator button to erase

all fingerprint information stored in the biometric lock and deny access to the owner and the other users of the safe without the consent of the owner. Thus, unrestricted access to the administrator button prevents the owner or administrator from having exclusive control over who has access to the safe.

[0008] Thus, there is a need in the art for a biometric safe lock that assists the user in properly aligning his or her biometric indicator on the biometric sensor. In addition, there is a need for a biometric safe lock that provides additional visual cues that assist a user in operating the lock and reduces the need to refer to a separate instruction manual. Further, there is a need for a biometric lock that allows an administrator to prevent the general users of the safe from accessing the administrator button positioned within the safe. The present invention fills these needs as well as other needs.

BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWINGS

[0009] The above-mentioned and other features and advantages of this invention, and the manner of attaining them, will become apparent and be better understood by reference to the following description of one embodiment of the invention in conjunction with the accompanying drawings, wherein:

[0010] FIG. 1 is a front perspective view of a biometric lock interface of the present invention;

[0011] FIG. 2 is a schematic view of a biometric lock of the present invention;

[0012] FIG. 3 is a flow chart showing the use and operation of the biometric lock when a valid user opens the safe;

[0013] FIG. 4 is a flow chart showing the use and operation of the biometric lock when a manager attempts to open the safe, enroll a fingerprint, or delete a fingerprint from the biometric lock;

[0014] FIG. 5 is a flow chart showing the use and operation of the biometric lock when an attempt is made to enroll a fingerprint;

[0015] FIG. 6 is a flow chart showing the biometric lock entering an administration mode;

[0016] FIG. 7 is a flow chart showing the operation of the biometric lock when access is denied;

[0017] FIG. 8 is a schematic drawing showing a lock cam member in a position to restrict access to an administration button; and

[0018] FIG. 9 is a schematic drawing similar to FIG. 8 showing a lock cam member engaging a safe actuator to unlock the safe, wherein the locking cam member is in a position to allow access to the administration button.

DETAILED DESCRIPTION OF THE INVENTION

[0019] Referring to the drawings and particularly FIGS. 1 and 2, there is shown a component of a biometric lock 8 that may include a biometric lock interface 10, which may be used to secure and restrict access to the internal compartment of a safe. In general, biometric lock 8 controls access to an internal compartment the safe by comparing a person's unique identifying characteristic of against one or more previously enrolled images for the purpose of recognition. Biometric interface 10 generally includes a body 12 that is mountable on the external surface of the safe. Biometric interface 10 may also include a display 14, a biometric sensor 16, an enter button 18, and a pair of

scroll buttons 20, 22. Further, biometric interface 10 may include transparent or other type of surfaces 24 located within a recess 33 and around the enter button 18 and scroll buttons 20, 22 that will allow light emitted from one or more backlight Light Emitting Diodes (LED's) 26 to pass therethrough. The light passing through surfaces 24, in conjunction with display 14, provides the user with visual cues to assist in operating biometric lock 8.

[0020] Biometric interface 10 may also include a biometric alignment feature 28 that is positioned relative to biometric sensor 16 to guide the user in properly positioning his or her unique identifying characteristic, such as a fingerprint, in an acceptable location on biometric sensor 16. Biometric alignment feature 28 may include one or more crosshairs 30, 32 that are positioned on the surface of body 12 to identify an acceptable target area for a user to place the thick or pad portion of his or her fingerprint on biometric sensor 16 so that biometric sensor 16 is able to read the fingerprint. In particular, crosshairs 30 may be aligned with each other, extend vertically, and positioned on opposite sides of biometric sensor 16, wherein one crosshair 30 is positioned above the top boundary of the sensor 16 and the other crosshair is positioned below the bottom boundary of the sensor 16. Crosshairs 32 may be aligned with each other, extend horizontally, and positioned on opposite sides of biometric sensor 16, wherein one crosshair 32 is positioned to the left of the left boundary of the sensor 16 and the other crosshair is positioned to the right of the right boundary of the sensor 16. It will be understood and appreciated that biometric alignment feature 28 may take other forms so long as the feature directs the user to properly position his or her unique identifying feature on biometric sensor 16 so that an adequate reading can be taken.

[0021] The present invention uses fingerprint identification as the identifying characteristic, therefore biometric sensor 16 may be either a capacitance or optical fingerprint sensor. While the present invention uses a person's fingerprint as the unique identifying feature that will unlock biometric safe 8, it will be understood that any unique identifying living or human characteristic, such as, but not limited to voice recordings, irises, facial images and the like may be read by biometric sensor 16. Biometric sensor 16 may be positioned within a recess 33 formed in body 12 of biometric interface 10. Moreover, body 12 may be constructed in such a way that the biometric interface 10 is angled upwardly relative to the surface of the safe so it is easier for a user to place his or her finger on biometric sensor 16, access the enter button 18 and scroll buttons 20, 22 and read the information set forth on display 14.

[0022] Display 14 may be a Liquid Crystal Display (LCD) screen that is adapted to provide visual clues or prompts to provide a user with instructions or information during operation of the biometric lock 8. The types of instructions or information that may be provided on display 14 include text prompts or symbols to provide directions to a user, a battery level indicator that informs the user of the power remaining in the biometric lock 8, and other information. Likewise, the visual cues provided to a user by the background LED's that selectively emit light on the biometric sensor 16 also provides direction to a user as to what steps are required to proceed with either gaining access to the safe or add/delete information from biometric lock 8.

[0023] As best seen in FIG. 2, biometric lock 8 includes biometric lock interface 10 and a power source 34 that are user accessible, In addition, biometric lock 8 includes an actuator printed writing board 36 and a safe actuator 38 that are not user accessible.

Biometric interface 10 includes a start or enter button 18 that is connected to one or more regulators and power source 34. Power source 34 may be in the form of a battery that provides the necessary power to operate all of the components of biometric lock 8. When the start or enter button 18 is initiated, power from power source 34 is directed to a controller 42. Controller 42 is a processor which includes memory for storing fingerprints and other types of information. Controller 42 is connected to display 14, backlight LED's 26 and a keypad matrix 44, which may be used to transfer input commands from a user through the use of scroll buttons 20, 22. Biometric sensor 16 is connected to a buffer 46 that is used to regulate the rate of flow of data between sensor 16 and controller 42. Biometric interface 10 also includes an alerter 47 that is connected to controller 42 and may be used to provide a visual, audible or other type of signals to a user. A reset 48 is connected to controller 42 which may be used to clear any fingerprint data or other type of information stored in the memory of controller 42. Reset 48 is connected to an administrator button 50 (FIGS. 8 and 9) that may be mounted to actuator printed wiring board 36 and accessed when the safe door is unlocked by an administrator with a key. Administrator button 50 is a feature of biometric lock 8 in that may be used to delete all of the authorized fingerprints stored in the biometric lock. Therefore, the present invention restricts access to internal administrator button 50 through the use of a key override locking mechanism 52, which will be discussed in more detail below. An oscillator 54 is connected to controller 42 and provides timing for the communication between controller 42 and a 128-bit serial shift register 56 located on actuator printed wiring board 36.

[0024] Shift register 56 is connected to controller 42 through the use of a four-wire interface 58. For security purposes, the communication between controller 42 and shift register may be encrypted in such a way that the voltage pulses are unique for each safe. Shift register 56 is connected to an identity comparator 60, which is turn connected to an actuator interface 62. Actuator interface 62 is connected to safe actuator 38 and provides the signals necessary to unlock the safe through the use of a solenoid or other type of locking mechanism.

[0025] A conventional locking mechanism may be mounted to the safe and be moved between locked and unlocked positions using a key to provide an alternative way of gaining access to the safe. In accordance with the present invention, key override locking mechanism 52 is associated with the conventional locking mechanism in such a manner to allow access to administrator button 50 when the key is turned to an unlocked position so that the memory of biometric lock 10 may be reset or cleared. It will be understood and appreciated that an administrator of biometric lock 8 is the person who has access to the key for the conventional locking mechanism.

[0026] As best seen in FIG. 8, administrator button 50 is positioned on actuator printed writing board 36. In addition, the conventional locking mechanism is coupled with key override locking mechanism 52 having a lock axis 64 that is adapted to rotate as the key is rotated between the locked and unlocked position. A cam member 66 is coupled with lock axis 64 and is adapted to rotate along with lock axis 64. When the conventional locking mechanism is positioned in a locked position, cam member 66 is positioned in such a way to cover or otherwise restrict access to administrator button 50. Therefore, if a general or non-administrator user gains access to the internal compartment

of the safe through the use of biometric lock 8, he or she will not be able to access to administrator button 50 as long as the conventional locking mechanism is in a locked position and cam member 66 is covering the administrator button 50.

[0027] As best seen in FIG. 9, conventional locking mechanism may be moved to a unlocked position through the use of a key. As the key is turned from the locked position (FIG. 8), lock axis 64 rotates counterclockwise, which also causes cam member 66 to rotate in a counterclockwise direction. As lock axis 64 and cam member 66 are rotated in a counterclockwise direction, cam member 66 depresses an actuator button 68 on actuator 38 to unlock the safe. Further, the rotation of cam member 66 operates to expose administrator button 50 and allow someone to reset or clear the fingerprint information stored in controller 42. Administrator button 50 may be used until the cam member 66 is positioned in such a way to restrict access to administrator button 50, such as in FIG. 8.

[0028] Biometric lock 8 has the capacity to store one or more fingerprints for two managers and six general users that are permitted access to the interior portion of the safe. A manager not only has the ability to gain access to the safe by using his or her fingerprint to open the biometric lock 8, the manager also has the authority to add and delete general users from the memory of biometric lock 8. As stated above, the administrator of biometric lock 8 is the person who has access to the key for the conventional locking mechanism, and thus may access administrator button 50 and reset or clear the memory in biometric lock 8. The general users of the biometric lock 8 only have the ability to gain access to the safe by using his or her fingerprint to open the biometric lock 8. The general users are not able add or delete any other general users or

managers, unless the general user is the administrator in which case the general user has the ability to access administrator button 50 and reset or clear the memory in biometric lock 8. Preferably, each of the managers and general users may be required to store two fingerprints (e.g., thumb and index fingerprint) in biometric lock 8 to gain access to the safe. However, it will be understood that more or less fingerprints may be required depending at least in part on the desired level of security for the safe. Further, it is within the scope of the present invention to include any number of managers or general users in biometric lock 8.

[0029] During an attempt to unlock, add or delete a fingerprint from biometric lock 8, biometric lock interface 10 performs a series of sequencing events that provides the user with visual cues, such as written information on display 14 and prompt LED's 26, to assist and provide the user with instructions for operating biometric lock 8. Biometric lock 8 may perform different sequencing events in situations where a valid user opens a safe (FIG. 3), a manager opens the safe or enrolls/deletes fingerprints from biometric lock 8 (FIGS. 4 and 5), entering an administration mode by using administration button 50 (FIG. 6), and a entry attempt where the biometric feature of the user does not match (FIG. 7).

[0030] As best seen in FIG. 3, biometric lock 8 may undergo a series of sequencing steps when a valid user attempts to open the safe. With additional reference to FIGS. 1 and 2, step 100 shows that the user may press the enter button 18 on biometric lock interface 10, which may direct power from battery to all of the components shown in FIG. 2. At that point, backlight LED's 26 operate to emit light through surfaces 24 to light up biometric sensor 16, scroll buttons 20, 22 and enter button 18. The backlight

LED's 26 also operate to illuminate display 14. Further, text may appear on display 14 giving an instruction to "Place Finger on Sensor" at step 102. Further guidance may be provided on display 14 by showing a symbol such as an arrow pointing toward the biometric sensor 16. At that point, the lighting and written information provided on display 14 directs the users attention to sensor 16. In placing the fingerprint on biometric sensor 16, biometric alignment feature 28 will be used to provide a target so that the fingerprint will be properly aligned on sensor 16. Proper alignment may be required to ensure that biometric lock 8 can obtain a proper fingerprint reading. Specifically, the user will use crosshairs 32 to vertically align the thick portion of the fingerprint on sensor 16, and use crosshairs 30 to horizontally align the thick portion of the fingerprint on sensor 16. In addition, the user may align his or her finger with crosshairs 30 so that the fingerprint is in a proper rotational position when placed on sensor 16. Once the user has properly placed one or more of his or her fingerprints on biometric sensor 16, the fingerprint information is sent to controller 42 to determine if the one or more fingerprints matches a previously stored fingerprint contained within the memory of controller 42. If the fingerprint of the user matches a stored fingerprint in controller 42, controller 42 may then send an encrypted signal to shift register 56. Shift register 56 then sends a signal to identity comparator 60 which sends a signal to actuator interface 62. Actuator interface 62 then activates safe actuator 38 at step 104 to unlock the safe and the biometric lock 8 shuts off at step 106. The user may then access the internal compartment of the safe and lock the safe by rotating a lock handle (not shown).

[0031] As best seen in FIGS. 4 and 5, biometric lock 8 may undergo a series of sequencing steps when a manager opens the safe, or wants to add or delete one or more

fingerprints from the biometric lock 8. With additional reference to FIGS. 1 and 2, step 200 shows that the user may press the enter button 18 on biometric lock interface 10, which may direct power from battery to all of the components shown in FIG. 2. At that point, backlight LED's 26 operate to emit light through surfaces 24 to light up biometric sensor 16, scroll buttons 20, 22 and enter button 18. The backlight LED's 26 also operate to illuminate display 14. Further, text may appear on display 14 giving an instruction to "Place Finger on Sensor" at step 202. Further guidance may be provided on display 14 by showing a symbol such as an arrow pointing toward the biometric sensor 16. At that point, the lighting and written information provided on display 14, directs the users attention to sensor 16. In placing the fingerprint on biometric sensor 16, alignment feature 28 will be used to provide a target so that the fingerprint will be properly aligned on sensor 16. Proper alignment may be required to ensure that biometric lock 8 can obtain a proper fingerprint reading. Specifically, the user will use crosshairs 32 to vertically align the thick portion of the fingerprint on sensor 16, and use crosshairs 30 to horizontally align the thick portion of the fingerprint on sensor 16. In addition, the user may align his or her finger with crosshairs 30 so that the fingerprint is in a proper rotational position when placed on sensor 16. Once the user has properly placed one or more of his or her fingerprints on biometric sensor 16, the fingerprint information is sent to controller 42 to determine if the one or more fingerprints matches a previously stored fingerprint contained within the memory of controller 42. If the fingerprint matches a stored fingerprint in controller 42, at least the backlight LED 26 emitting light on sensor 16 may shut off indicating that a valid fingerprint has been read by controller 42. At that point, the controller 42 may then send an encrypted signal to shift register 56. Shift

register 56 then sends a signal to identity comparator 60 which sends a signal to actuator interface 62. Actuator interface 62 then activates safe actuator 38 at step 204 to unlock the safe.

[0032] Furthermore, after biometric lock 8 recognizes the one or more fingerprints corresponds to one or more of the managers, text may appear on display 14 giving an instruction to "Press ENTER to enroll/delete" at step 206. If the manager would like to add/delete a fingerprint stored in the memory of controller 42, the manager may press the enter button 18 at step 208. The display 14 will then show text that make up one or more selections that may include "Usr 1 Finger 1*, Usr 1 Finger 2, Usr 2 Finger 1*, Exit, etc. . ." at step 210. The asterisk ("*") positioned in association with a selection indicates that fingerprint information is stored in the memory assigned to that particular selection. Therefore, if the manager wants to add or enroll a new fingerprint in a memory location (Usr 1 Finger 1*) that already has a fingerprint stored therein, manager may be required to delete the fingerprint information that is stored in the memory location. The manager may delete a stored fingerprint by locating the memory location that he or she wants to delete by scrolling through the available memory locations with scroll buttons 30, 32 and selecting, for example, "Usr 1 Finger 1*" using the enter button 18 at step 212. At step 214, display 14 may then display the selected memory location (i.e., Usr 1, Finger 1) and ask the manager whether this is the fingerprint that should be deleted using "YES" and "NO" selections that may be scrolled through by the manager using buttons 20, 22. If the manager selects "NO" at step 214, the sequencing will return to step 210. If the displayed fingerprint is the one that is to be deleted, the manager selects "YES" by pressing the enter button 18 at step 216. The

fingerprint stored in the memory of controller 42 will then be deleted. At step 218, the display 14 will then confirm that the deletion has taken place by displaying text that reads "Usr 1 Finger 1: DELETED." At that point, the sequencing of biometric interface 10 will return to step 210.

[0033] At step 210, the manager may also enroll a new fingerprint in a memory location (Usr 1 Finger 2) that does not have a fingerprint stored therein, or in a location in which a fingerprint has been deleted. The manager may add a fingerprint to the controller 42 memory by locating the memory location that he or she wants to store a new fingerprint by scrolling through the available memory locations with scroll buttons 30, 32 and selecting, for example, "Usr 1 Finger 2" using the enter button 18 at step 220. At step 222, display 14 may then display the selected memory location (i.e., Usr 1, Finger 2) and ask the manager whether this is the location in which the fingerprint should be added using "YES" and "NO" selections that may be scrolled through by the manager using buttons 20, 22. If the manager selects "NO" at step 222, the sequencing will return to step 210. If the displayed fingerprint storage location is the desired location for storing the added fingerprint, the manager selects "YES" by pressing the enter button 18 at step 224. The fingerprint may then be stored in the memory of controller 42 by proceeding through one or more sequencing events in step 226. At step 226, the biometric lock 8 requests the biometric and may proceed to enroll the fingerprint through a series of steps described in FIG. 5.

[0034] As best seen in FIG. 5, the display 14 may show text that directs the manager to "Place finger on sensor" at step 228. Further, display 14 may also have symbols such as arrows that and backlight LED 26 may be turned on to emit light on

sensor 16 to direct the managers attention to the biometric sensor 16. The manager may then place his or her fingerprint on biometric sensor 16 so that an initial reading can be taken at step 230. The display 14 will then display text that reads "Lift then replace finger" at step 232 and the biometric interface 10 may provide additional visual cues, such as lighting, to direct the manager to place his or her fingerprint on biometric sensor 16. The manager may then place his or her fingerprint on biometric sensor 16 so that second reading can be taken at step 234. The display 14 will then display text that reads "Again lift then replace finger" at step 236 and the biometric interface 10 may provide visual cues to direct the manager to place his or her fingerprint on biometric sensor 16 for a third reading. The manager may then place his or her fingerprint on biometric sensor 16 so that the third reading can be taken at step 238. If the image quality of all the fingerprint readings were adequate, display 14 will show text that reads "Finger successfully enrolled" for three seconds at step 240 and then proceed back to step 210 in FIG. 4.

[0035] If the image quality of any of the fingerprints taken at any one of steps 230, 232, 238 is not adequate, display 14 may show text that reads "-Unsuccessful- Try Again: Note position and firmness" at step 244. The manager will then replace his or her finger on biometric sensor 16 at step 246 and proceed with the enrollment process at the next successive step, i.e., step 232, 236 or 240. If too many poor images are obtained by biometric lock 8, enrollment may fail at step 248 and display 14 may show text that reads "Enrollment failed: Clean sensor and try again." The sequencing will then proceed to step 210 in FIG. 4.

[0036] As best seen in FIG. 7, the biometric lock also has a sequencing that it undergoes for an entry attempt where a biometric does not match. As with the other sequencing events, the biometric lock 8 is initiated by using the enter button 18 on biometric interface 10. In particular, with additional reference to FIGS. 1 and 2, step 300 shows that the user may press the enter button 18 on biometric lock interface 10, which directs power from battery to all of the components shown in FIG. 2. At that point, backlight LED's 26 operate to emit light through surfaces 24 to light up biometric sensor 16 scroll buttons 20, 22 and enter button 18. The backlight LED's 26 also operate to illuminate display 14. Further, text may appear on display 14 providing an instruction to "Place Finger on Sensor" at step 302. Further guidance may be provided on display 14 by showing a symbol such as an arrow pointing toward the biometric sensor 16. At that point, the lighting and written information provided on display 14 directs the users attention to sensor 16. After the fingerprint is read by biometric sensor 16 and controller 42 does not recognize the user as one of the fingerprints stored therein, display 14 may show text that reads "NO MATCH: Try Again" at step 304. At step 306, the fingerprint is then replaced on biometric sensor 16 and compared with the fingerprints stored in the memory of controller 42. If the fingerprint does not match any of the stored fingerprints, display 14 may show text that reads "NO MATCH: Try Again" at step 308. In a third or final attempt to gain access to the safe, the fingerprint is again placed on biometric sensor 16 at step 310. If the controller 42 does not recognize the fingerprint during this third and final attempt, display 14 may show text that reads "ACCESS DENIED" at step 312 and biometric lock 8 may self-disable for a period of time, for example, 30 seconds, at step 314. While the present sequencing example allows for three chances to enter a valid

fingerprint in steps 302, 306, 310, it will be understood that more or less chances may be implemented.

[0037] In order to access the administration mode that will allow all of the fingerprints stored in the controller 42 memory to be deleted or erased, the steps shown in FIG. 6 may be followed. First, the administrator uses a key to unlock the conventional locking mechanism, which enables the administrator to bypass the biometric lock 8 and gain access to the internal compartment of the safe. As the administrator is moving the conventional locking mechanism from a locked position to an unlocked position, lock axis 64 and cam member 66 are rotated counterclockwise, as best seen in FIGS. 8 and 9, thereby rotating cam member 66 allows access to administration button 50. With administrator button 50 being in an exposed position, the administrator may then press administration button 50 at step 402 to erase all of the fingerprints stored in the memory of controller 42. The sequencing of biometric lock 8 would then move to step 210 in FIG. 4 as described above.

[0038] The present invention overcomes and ameliorates the drawbacks and deficiencies in the prior art. Specifically, the biometric lock of the present invention includes a number of visual cues, such as instructions and symbols provided on a display, prompt LED's, and a biometric alignment feature, to make the unlocking of the safe easier and more efficient than a safe equipped with existing biometric locks. Moreover, the present invention includes a key override locking mechanism that prevents users who are not administrators of the biometric lock from erasing all of the fingerprints stored in the controller memory and taking control of the biometric lock.

[0039] Although the present invention has been described in considerable detail with reference to certain preferred versions thereof, other versions are possible. Therefore, the spirit and scope of the appended claims should not be limited to the description of the preferred versions contained herein.

[0040] All features disclosed in the specification, including the claims, abstract, and drawings, and all the steps in any method or process disclosed, may be combined in any combination, except combinations where at least some of such features and/or steps are mutually exclusive. Each feature disclosed in the specification, including the claims, abstract, and drawings, can be replaced by alternative features serving the same, equivalent or similar purpose, unless expressly stated otherwise. Thus, unless expressly stated otherwise, each feature disclosed is one example only of a generic series of equivalent or similar features.

CLAIMS

What is claimed is:

1. A biometric lock interface used with a biometric lock to secure an enclosure, the biometric lock interface comprising:

a body;

a biometric sensor mounted to the body for reading a unique identifying feature of an individual; and

a biometric alignment feature associated with the sensor to assist a user in properly positioning the unique identifying feature on the sensor.

2. The biometric lock interface recited in claim 1, wherein the biometric alignment feature includes at least one crosshair.

3. The biometric lock interface recited in claim 2, wherein the sensor is rectangular, wherein the biometric alignment feature includes a first pair of crosshairs positioned on opposite sides of the sensor, and a second pair of crosshairs positioned on opposite sides of the sensor, wherein first and second sets of crosshairs provide a guide for placement of the unique identifying feature.

4. The biometric lock interface recited in claim 3, wherein first and second pairs of crosshairs intersect in a central location of the sensor.

5. The biometric lock interface recited in claim 1, further comprising:

a light emitting mechanism associated with the biometric sensor for selectively illuminating the biometric sensor.

6. The biometric lock interface recited in claim 5, wherein the a light emitting mechanism is an Light Emitting Diode (LED).

7. The biometric lock interface recited in claim 5, wherein the body includes a first portion that is formed of a material that allows light to pass therethrough, wherein the light given off by the light emitting mechanism is directed through the first portion and onto biometric sensor.

8. The biometric lock interface recited in claim 1, further comprising a display coupled with the body for conveying information to a user of the biometric lock.

9. An enclosure having an interior compartment that may be accessed through a door hingedly mounted to a body of the enclosure, the enclosure comprising:

a biometric lock coupled with the enclosure that may be used to lock and unlock the door of the enclosure, the biometric lock having a biometric lock interface and a controller, the biometric lock interface having a biometric sensor mounted to the body for reading a unique identifying feature of an individual, the controller is connected to the biometric sensor and has the capacity to store at least one fingerprint read by the biometric sensor in a memory location, wherein

the biometric lock includes an administrator button for clearing the fingerprint information stored in the memory location;

a key lock coupled to the enclosure to lock and unlock the door of the enclosure, the key lock including a cam member that is positioned in such a way to restrict access to the administrator button when the key lock is in a locked position, and allows access to the administrator button when the key lock is in an unlocked position, wherein the biometric lock and the key lock independently operate to lock and unlock the door of the enclosure.

10. The enclosure recited in claim 9, wherein the key lock includes a lock axis, wherein the cam member and the lock axis are fixedly coupled to one another.

11. A method for unlocking a safe using a biometric lock, the biometric lock including a locking mechanism and a biometric lock interface having a biometric sensor and a display, the method comprising:

initiating the biometric lock using the biometric lock interface;

providing a visual cue to a user to place a unique identifying feature on the biometric sensor;

placing a unique identifying feature on the biometric sensor; and

comparing the unique identifying feature with a unique identifying feature of an authorized user, wherein the safe is unlocked if the unique identifying feature matches the unique identifying feature of an authorized user, and wherein

the safe remains locked if the unique identifying feature does not match the unique identifying feature of an authorized user.

12. The method of claim 1, wherein the visual cue is information displayed on the display.

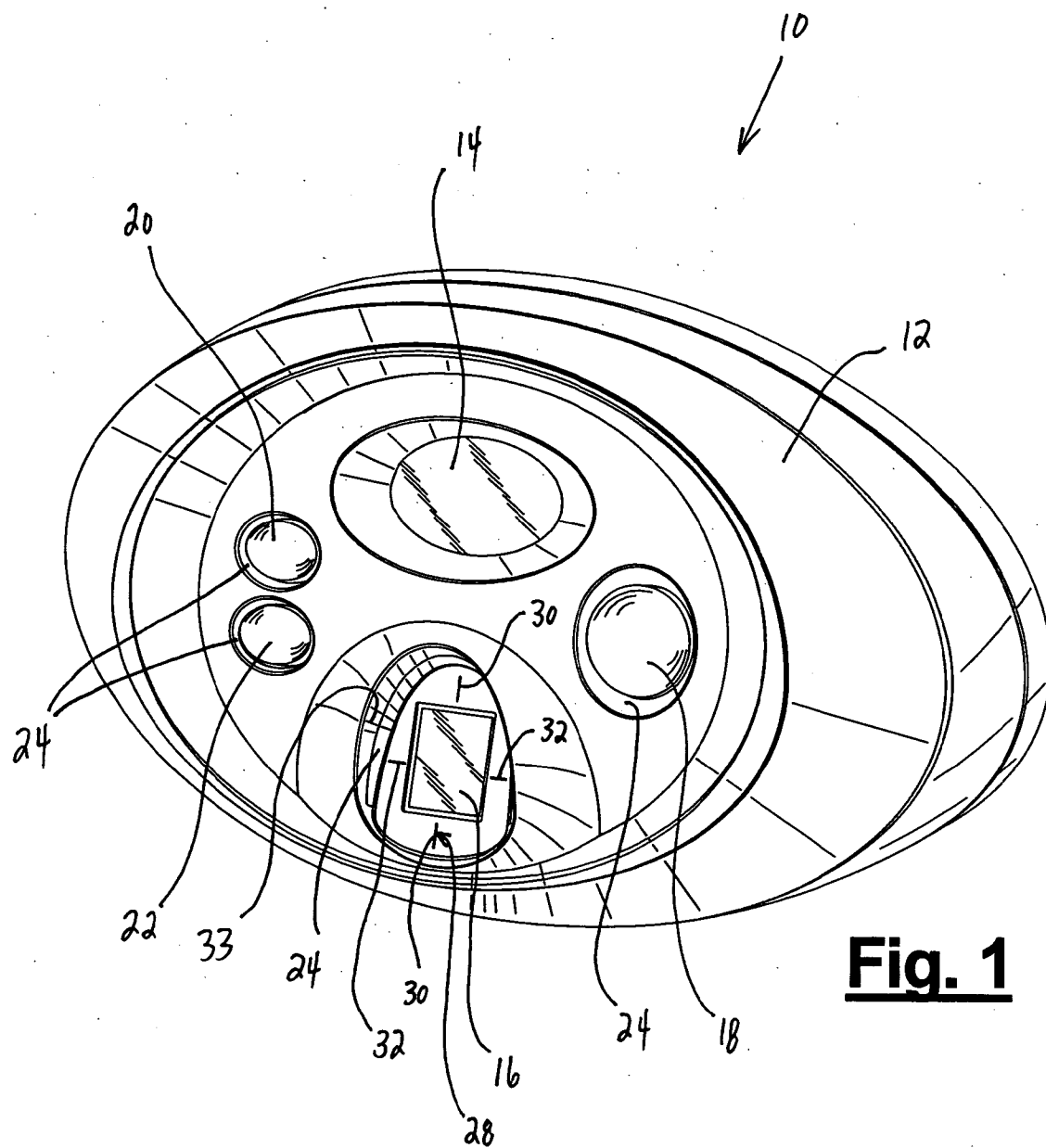
13. The method of claim 12, wherein said information is at least one word.

14. The method of claim 12, wherein said information is at least one symbol.

15. The method of claim 1, wherein the visual cue is light emitted onto the biometric sensor.

16. The method of claim 1, wherein the visual cue is a biometric alignment feature positioned in association with the biometric sensor.

17. The method of claim 16, wherein the biometric alignment feature is at least one crosshair.



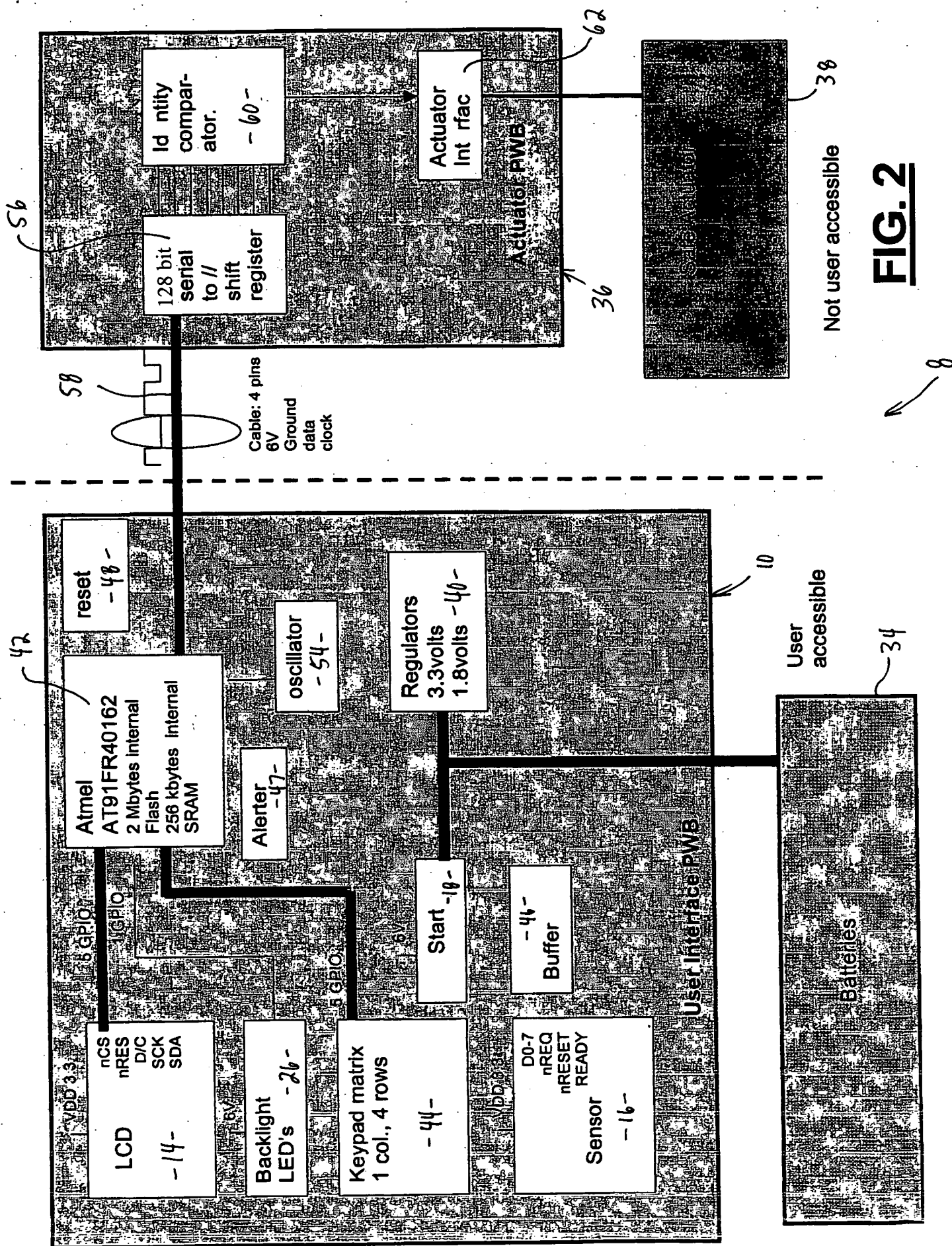


FIG. 2

1. Valid user opening safe.

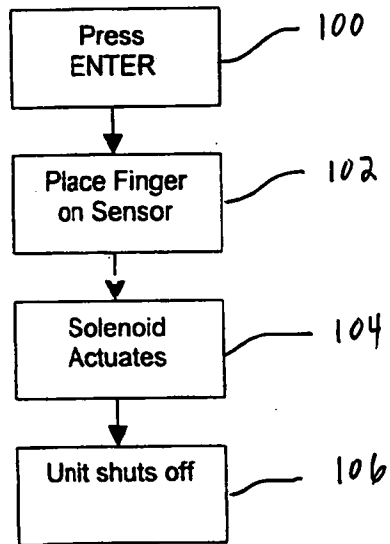


FIG. 3

2. Manager Opening Safe, enrolling/deleting fingers

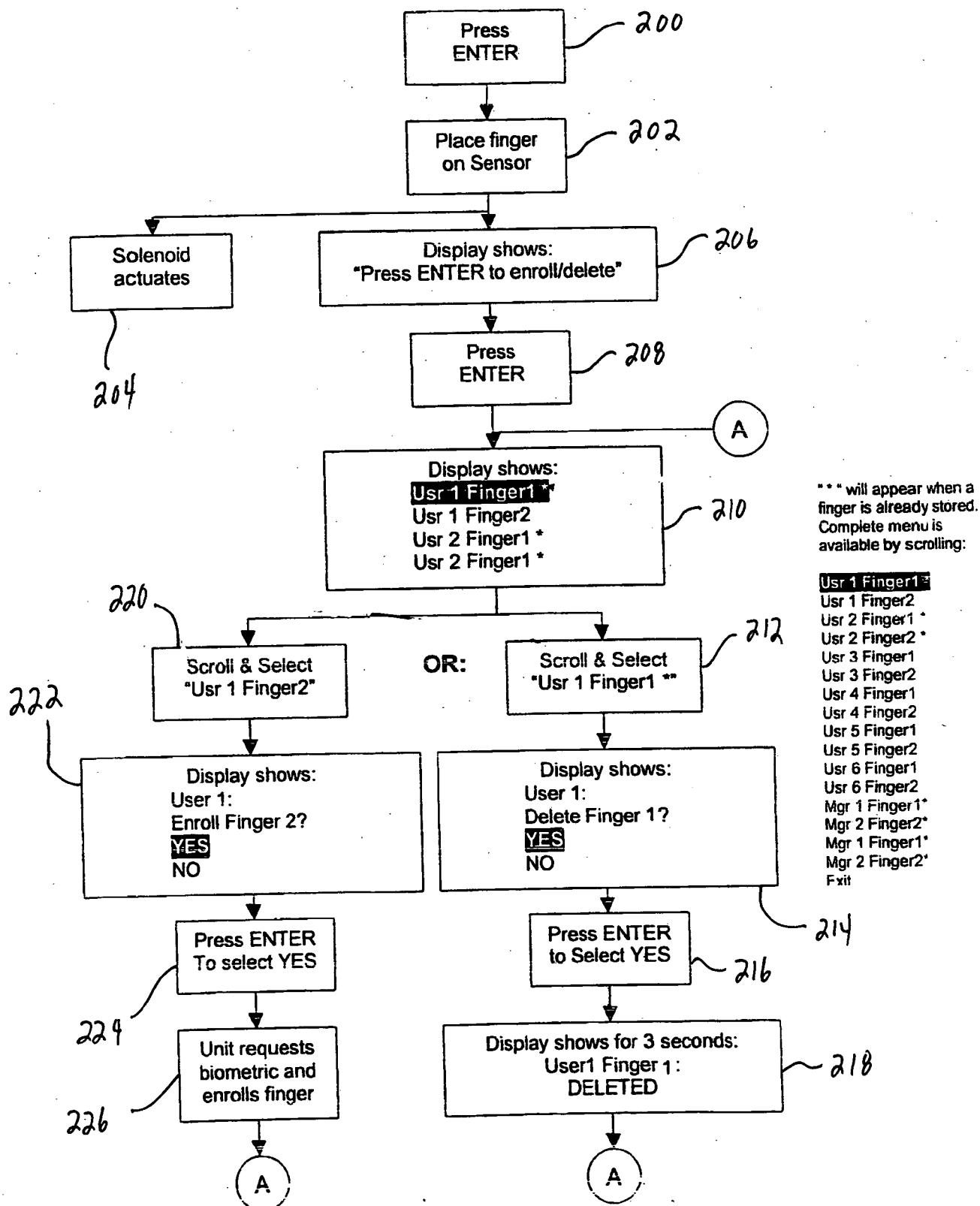


FIG. 4

3. Enrolling a finger

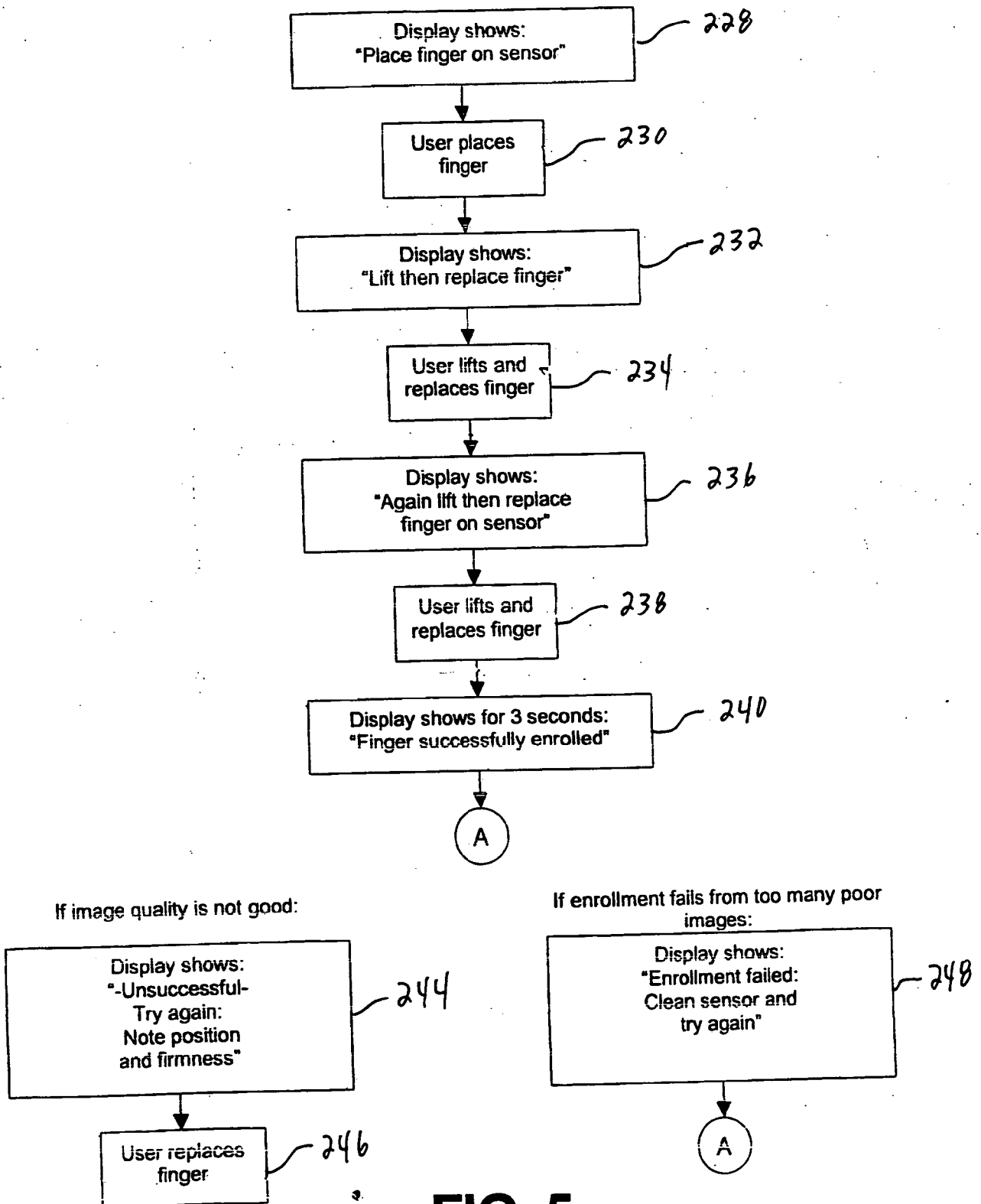


FIG. 5

4. Entering Administration mode from the internal button

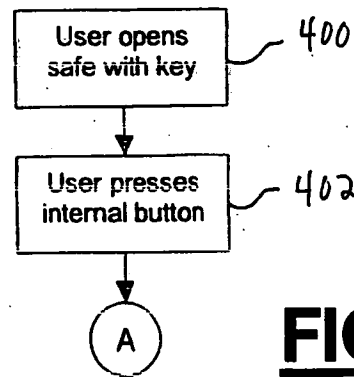


FIG. 6

5. Entry attempt: Biometric does not match

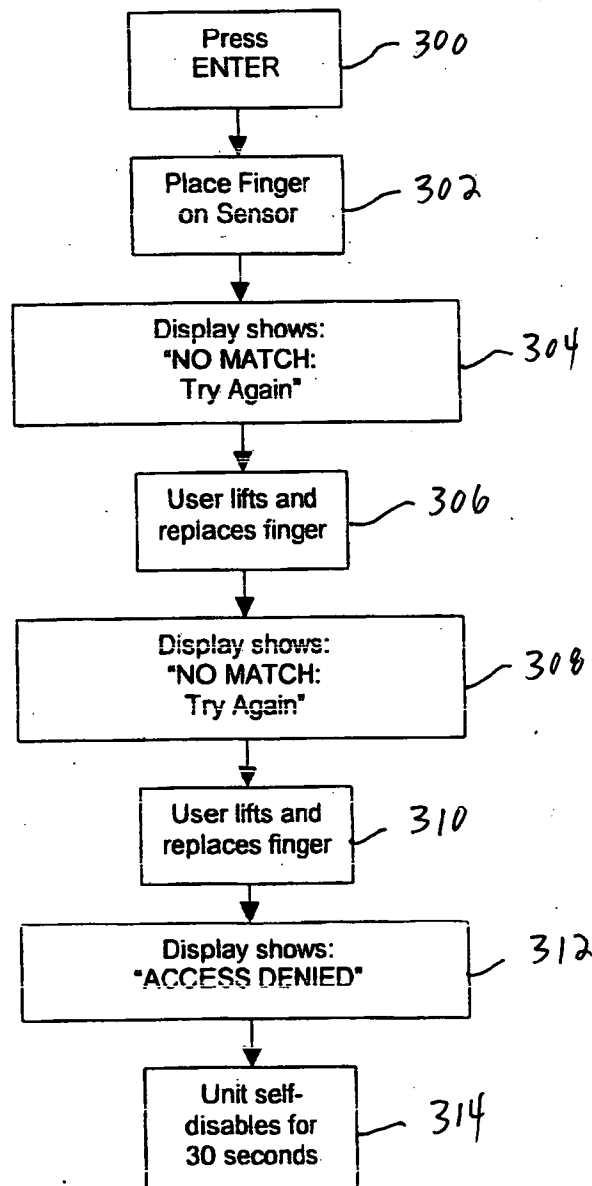


FIG. 7

